State of Arizona

Department of Economic Security Information Technology Standards	Title: 1-38-0045 Authentication Policy

Subject: This policy defines authentication methods that must be used when accessing DES systems.	***Effective Date:*** **04/03/03**	***Revision:*** 1.1

1. **Summary of Policy Changes**
   1.1. 10/29/04 – Addition by the DTS Information Security Administration of 6.5, about employees' authentication from a remote site, and that vendors must also enforce strong two-factor authentication when hosting DES data,

2. **Purpose**
   This policy defines authentication methods that must be used by DES employees and all others with access to DES IT facilities or systems.

3. **Scope**
   This policy applies to all DES administrative entities, councils, divisions, administrations, and programs.

4. **Responsibilities**
   4.1. The DES Director, Deputy Directors, Associate Director, and Assistant Directors are responsible for implementing and enforcing this policy.
   4.2. The DES CIO and the DES Division of Technology Services are responsible for implementing this policy.
   4.3. All DES Managers and Supervisors are responsible for monitoring compliance to this policy.

5. **Definitions and Abbreviations**
   5.1. **Definitions**

   5.1.1. **PKI – P**ublic **K**ey **I**nfrastructure enables users of a non-secure public network, such as the Internet, to securely exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. PKI provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.

   5.1.2. **VPN –** A **V**irtual **P**rivate **N**etwork is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

   5.1.3. **SecurID Fob –** SecurID is a proprietary authentication technology that uses a small electronic device called a "fob". The fob displays a password that changes periodically, and is synchronized with a password generator in the network at the authentication point.

   5.2. **Abbreviations**
   5.2.1. **ADOA**- **A**rizona **D**epartment **o**f **A**dministration
   5.2.1. **CIO – C**hief **I**nformation **O**fficer
   5.2.2. **DTS – D**ivision of **T**echnology **S**ervices
   5.2.3. **DES – D**epartment of **E**conomic **S**ecurity

5.2.4. **GITA – G**overnment **I**nformation **T**echnology **A**gency

5.2.6. **PC – P**ersonal **C**omputer

6. POLICY

6.1. All remote access to DES systems, with the exception of the Public accessing DES web sites, requires a second level of authentication. SecurID “fobs”, which are already used by several DES divisions, are an example of such authentication.

6.2. Current exceptions to this policy are DES employees accessing e-mail and the short-term use of the ADOA VPN.

6.3. Another exception may be the use of a “Password and PIN” scheme to authenticate clients entering applications through the Internet. This practice must be approved by the appropriate DES Assistant Director and the DES CIO before it may be implemented.

6.4. A “password only” authentication method is not sufficient to protect DES systems and data.

6.5. Employees accessing DES data on a remote site must also use a two-factor authentication scheme. In other words, vendors must also enforce strong two-factor authentication when hosting DES data.

6.6. Public Key Infrastructure (PKI) provides very effective authentication and an electronic signature facility recognized by Federal and State law. DES will eventually implement services requiring enhanced authentication, but in the short term, PKI should be limited to, and be required for, scenarios that require electronic signatures.

6.7. Other uses of PKI may be implemented with the prior approval of the appropriate DES Assistant Director and the DES CIO

6.8. DES programs and divisions will pay for all authentication devices and authentication software used by DES employees.

6.9. In order to remain effective, authentication devices like PKI certificates and SecurID “fobs” must be controlled by DES. DES will control the security devices used by other agencies, stakeholders, and the Public, but may charge those users for the service.

7. Implications

7.1. Some programs and divisions will need to improve their current authentication practices.

8. Implementation Strategy

8.1. All DES business entities should immediately begin to comply with this policy.

9. References

9.1. 1-38-0005 DES Remote Access Authentication Standard

9.2. 1-38-0043 DES Remote Access & Telecommuting Policy

9.3. 1-38-0046 DES Remote Access Network, Server, and PC Support Policy

10. Attachments

10.1. None

11. Associated GITA IT Standards or Policies

11.1. None

12. Review Date

12.1 This document will be reviewed twelve (12) months from the original adoption date and every twelve months thereafter.